FORM PTO-1390 (REV 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: PA1066US

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/555408 Unknown

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US99/24191	October 14, 1999	October 14, 1999

TITLE OF INVENTION: System And Method OF Sending And Receiving Secure Data Using Anonymous Keys

APPLICANT(S) FOR DO/EO/US: Lynn D. Soraggs

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C371(b) and PCT Articles 22 and 39(1).
4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [X] is not required, as the application was filed in the United States Receiving Ofice (RO/US).
6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [X] Amendments to the claims of the International Application under PCT Article 19(35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:

    Small Entity Statement; Petition to Make Special Because of Prospective Manufacture; Statement in Support of Petition to Make Special; Petition Fee ($130)

U.S. APPLICATION NO (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/555408	PCT/US99/24191	PA1066US

	CALCULATIONS PTO USE ONLY
17. ☐ The following fees are submitted:	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):	
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO..... **$840.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$670.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 690.00
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 0.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	16 - 20 =	0	X **$18.00**	$ 0.00
Independent claims	4 - 3 =	1	X **$78.00**	$ 78.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$260.00**	$ 0.00
TOTAL OF ABOVE CALCULATIONS =				$ 768.00
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statment must also by filed (Note 37 CFR 1.9, 1.27, 1.28).				$ 384.00
SUBTOTAL =				$ 384.00
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$
TOTAL NATIONAL FEE =				$ 384.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00
TOTAL FEES ENCLOSED =				$ 424.00
			Amount to be refunded:	$
			charged:	$

a. ☒ A check in the amount of $ 424.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pendin g status.

SEND ALL CORRESPONDENCE TO:

Aaron R. Wininger
Carr & Ferrell LLP
2225 East Bayshore Road Suite 200
Palo Alto, CA 94303

SIGNATURE:

Aaron R. Wininger
NAME

45,229
REGISTRATION NUMBER

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Lynn D. Spraggs
SERIAL NO.:	Unknown
FILING DATE:	Unknown
INTL. APP. NO.:	PCT/US99/24191
INTL. FILING DATE:	October 14, 1999
TITLE:	System and Method of Sending and Receiving Secure Data Using Anonymous Keys
ATTY.DKT.NO.:	PA1066US

THE ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to examination, please amend the application as follows:

In the Specification:

On page 3, line 14, delete "not" and substitute -- now --.

REMARKS

By this Amendment, Applicant has provided a minor change to the specification. No new matter is being added. In the event that the Examiner has

any questions, he or she is respectfully invited to contact the undersigned at the number set out below.

Respectfully submitted,

Lynn Spraggs

Date: 5/25/00

By: _____

Aaron Wininger, Reg. No. 45,229
Carr & Ferrell LLP
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
(650) 812-3465

Atty. Dkt.No. PA1066US

Applicant: Lynn Spraggs
PCT International Serial No.: PCT/US99/24191
PCT Filed: October 14, 1999
US Serial No. Unknown
For: System and Method of Sending and Receiving Secure Data Using Anonymous Keys

VERIFIED STATEMENT (DECLARATION) CLAIMING
SMALL ENTITY STATUS
(37 CFR 1.9 (f) and 1.27 (c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

[ ] the owner of the small business concern identified below:
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN Aegis Systems Inc.
ADDRESS OF CONCERN 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.2, and reproduced in 37 CFR 1.9 (d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled "System and Method of Sending and Receiving Secure Data Using Anonymous Keys", by inventor Lynn Spraggs, as described in

[ ] the specification filed herewith.
[X] PCT application serial no. PCT/US99/24191, filed October 14, 1999.
[ ] patent no._____, issued _____.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME _____

ADDRESS _____

[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of the Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING ASHOK MATHUR

TITLE OF PERSON IF OTHER THAN OWNER PRESIDENT

ADDRESS OF PERSON SIGNING 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

SIGNATURE _____ DATE 4/27/00

Rec'd PCT/PTO 25 MAY 2000 09/555408
WO 00/22496 PCT/US99/24191

SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA USING ANONYMOUS KEYS

BACKGROUND OF THE INVENTION

1. Field of the invention

The present invention relates generally to computer security and more specifically to allow the secure transfer and receipt of data between computers using anonymous keys.

2. Description of the Prior Art

In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as

RSA) by a certificate authority. The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

Public key cryptography generally requires a large mathematical decomposition in order to work effectively. Generally, the length of a private key is in the order of 64 bytes. Decomposing these relatively small private keys requires considerable computational power. Public key cryptography is typically used as a one-way encryption and if a private key is changed, then everyone else that has the public key counterpart must receive a new public key.

Thus, it would be desirable to provide a system and method of securing data that is easy to use, allows a user to have only a private key unknown to anyone else, does not require a public key, allows for a larger size private key for high security, uses less computation power than public key cryptography, and can be used in two directions.

SUMMARY OF THE INVENTION

A system and method is provided of securely transmitting data between two computers over a network, such as the Internet, using anonymous keys that are private only to each user and are not shared with anyone else. The data is first encrypted at a first computer with a first private key into a first encrypted data file. The first encrypted data file is then transmitted to a second computer, wherein the first encrypted data file is encrypted with a second private key into a second encrypted data file. The second encrypted data file is then sent to the first computer, wherein the second encrypted data file is now decrypted with the first private key, known to the user at the first computer, into a third encrypted data file. The third encrypted data file is then sent to the second computer, wherein the third encrypted data file can not be fully decrypted into the original data file using the second private key.

Associative properties of encryption and decryption are used and allow for the use of large private keys in order to obtain a high-level of security. Additionally, the computational power to encrypt and decrypt data is significantly lower than the public key system since the encryption method is based on one private key and not on a public key and private key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a client transmitting secure data to a server over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the server computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the server computer of FIG. 2; and

FIG. 4 is a block diagram of the client computers shown in FIG. 1, in accordance with the present invention;

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module located within the client computers of FIG. 4; and

FIG. 6 is a flowchart of a method illustrating how a client, having a private key, passes encrypted data to a server computer, according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a client computer 102 through the Internet 106 using anonymous keys that are private and unknown to others.

FIG. 2 is a block diagram of the server computer 100 shown in FIG. 1. Server 100 includes a CPU 202, a RAM 204, a non-volatile memory 206, an input device 208, a display 210, and an Internet interface 212 for providing access to the Internet.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the server computer 100 of FIG. 2. The non-volatile memory 206 includes an encrypt/decrypt engine 302, and a secure data database 304 for storing secured data.

The encrypt/decrypt engine 302 is programmed to encrypt and decrypt data using a password or a key provided by the user. The encryption/decryption engine is programmed to use associative properties that would provide an associative-type of algorithm for the encryption and decryption of data. For example, if the data is encrypted by 'X' then that would result in encrypted data(X). If encrypted data(X) is then encrypted by 'Y' then that would result in encrypted data(X*Y). If encrypted data(X*Y) is decrypted by 'X' then that would result in encrypted data(Y). If encrypted data(Y) is decrypted by 'Y' then that would result in obtaining the original un-encrypted data. The computation power required to encrypt and decrypt data using this system and method is much less than the computational power required in a public/private key system, therefore longer keys can be used to provide an extremely high-level of security.

FIG. 4 is a block diagram of a client computer 102 shown in FIG. 1. Client 102 includes a CPU 402, a RAM 404, a non-volatile memory 406, an input device 408, a display 410, and an Internet interface 412 for providing access to the Internet.

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 404 located within the client 102 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404, and excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the client 102, thereby eliminating the need for the client to install his own encrypt/decrypt engine on his hard drive.

FIG. 6 is a flowchart of a method illustrating how a client, with a private key, passes data securely encrypted to a server computer through the Internet in accordance with the invention. It is not necessary for the data to pass to a server computer, it can equally work between two client computers. The process begins at step 600. A user enters data on the client computer at step 602. At step 604 the data is encrypted with the encrypt/decrypt engine using the user's private key (E1) and the once-encrypted data (D1) is sent over the Internet to the server.

At step 606 the server encrypts the once-encrypted data with the server private key (E2) and the twice-encrypted data [(D1)*(D2)] is sent back to the client over the Internet. At step 608 the client re-enters his private key and decrypts the twice-encrypted data with his private key resulting in once-encrypted data (D2) that is encrypted with the server private key. The once-encrypted data (D2) is sent over the Internet back

to the server. At step 610 the server can decrypt the once-encrypted data with the server private key (E2) to obtain full access to the original data fully decrypted. The server can then store the data in a secure data database 304 or process the data accordingly. The process then ends at step 612.

Various different modifications can be made to this invention, however, it is essential that the original data is encrypted at least twice, preferably with different private keys, prior to decrypting the data. Furthermore, the data must be sent back-and-forth between the client and server at least three times. This invention is ideal for transmitting small amounts of data, such as a personal identification number, however, the applications of this invention increase as the speed of transmission between computers increases.

The private key of both the client and server is not known by anybody else, therefore, the private key can be different every time a user utilizes this system and method of transmitting data. The private keys can also be very long (i.e. 1000 bytes) and could include biometric data, such as a digitized fingerprint of the user. Since this secure system and method of transmitting encrypted data utilizes a totally private key unknown to others, the various different applications of this invention are virtually limitless. Furthermore, the encrypted data would be virtually impossible to decrypt by a hacker since private keys can be

much longer than a typical private key (64 bytes) used in a private/public key system.

I Claim:

1. A system of encrypting and decrypting data using private keys for secure transmission, comprising:

an encrypt and decrypt engine for encrypting and decrypting data with a private key using associative properties of encrypting and decrypting, wherein said encrypt and decrypt engine can encrypt an unsecured data file with a first private key into a first encrypted file, encrypt the first encrypted data file with a second private key into a second encrypted file, decrypt the second encrypted file with the first private key into a third encrypted file, and decrypt the third encrypted file with the second private key into the unsecured data file.

2. The system of claim 1, wherein the private keys contain biometric data identifying its user.

3. A method of encrypting, decrypting and transmitting data using private keys for secure transmission from a first computer to a second computer, comprising the steps of:

providing unsecured data for transmission at the first computer;

encrypting the unsecured data using a first private key into a first encrypted data file;

transmitting the first encrypted data file to the second computer;

encrypting the first encrypted data file using a second private key into a second encrypted data file;

transmitting the second encrypted data file to the first computer;

decrypting the second encrypted data file using the first private key into a third encrypted data file;

transmitting the third encrypted data file to the second computer; and

decrypting the third encrypted data file using the second private key into the unsecured data.

4. The method of claim 3, further including the step of storing the unsecured data on the second computer.

5. The method of claim 3, further including the step of verifying the validity of the unsecured data after decrypting the third encrypted data file at the second computer.

6. The method of claim 3, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption.

7. The method of claim 3, wherein the private keys can include digitized biometric data identifying its user.

8. The method of claim 3, further including the step of processing the unsecured data after decrypting the third encrypted data file at the second computer.

9. A method of encrypting and decrypting data using private keys for secure transmission from a first computer to a second computer, comprising the steps of:

encrypting unsecured data using a first private key into a first encrypted data file at the first computer;

encrypting the first encrypted data file using a second private key into a second encrypted data file at the second computer;

decrypting the second encrypted data file using the first private key into a third encrypted data file at the first computer; and

decrypting the third encrypted data file using the second private key into the unsecured data at the second computer.

10. The method of claim 9, further including the step of storing the unsecured data on the second computer.

11. The method of claim 9, further including the step of verifying the validity of the unsecured data after decrypting the third encrypted data file at the second computer.

12. The method of claim 9, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption.

13. The method of claim 9, wherein the private keys can include digitized biometric data identifying its user.

14. The method of claim 9, further including the step of processing the unsecured data after decrypting the third encrypted data file at the second computer.

15. A computer-readable medium comprising program instructions for encrypting and decrypting data using private keys for secure transmission from a first computer to a second computer, comprising the steps of:

encrypting unsecured data using a first private key into a first encrypted data file at the first computer;

encrypting the first encrypted data file using a second private key into a second encrypted data file at the second computer;

decrypting the second encrypted data file using the first private key into a third encrypted data file at the first computer; and

decrypting the third encrypted data file using the second private key into the unsecured data at the second computer.

16. The method of claim 15, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption.

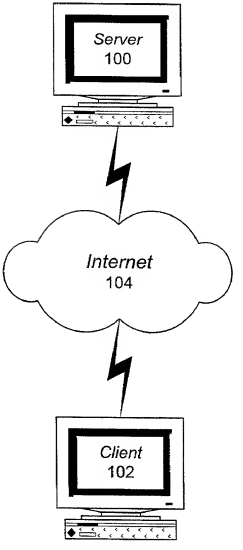

FIG. 1

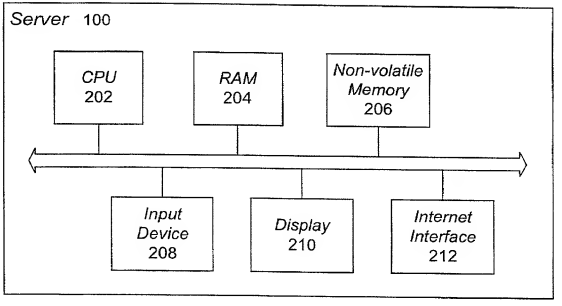
Server 100
CPU 202
RAM 204
Non-volatile Memory 206
Input Device 208
Display 210
Internet Interface 212

FIG. 2

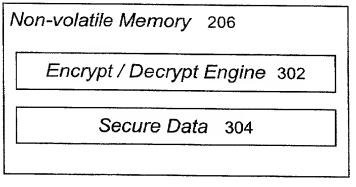
Non-volatile Memory 206
Encrypt / Decrypt Engine 302
Secure Data 304

FIG. 3

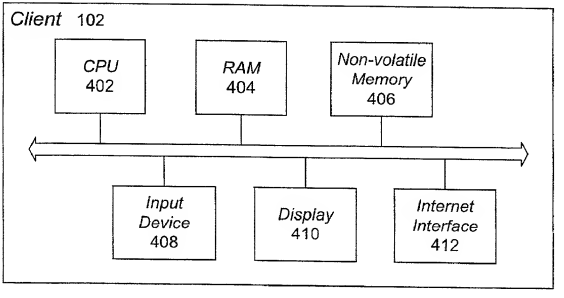
Client 102
CPU 402
RAM 404
Non-volatile Memory 406
Input Device 408
Display 410
Internet Interface 412

FIG. 4

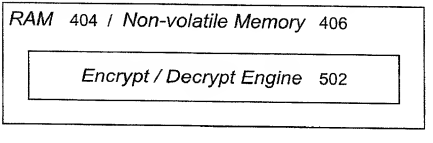
RAM 404 / Non-volatile Memory 406
Encrypt / Decrypt Engine 502

FIG. 5

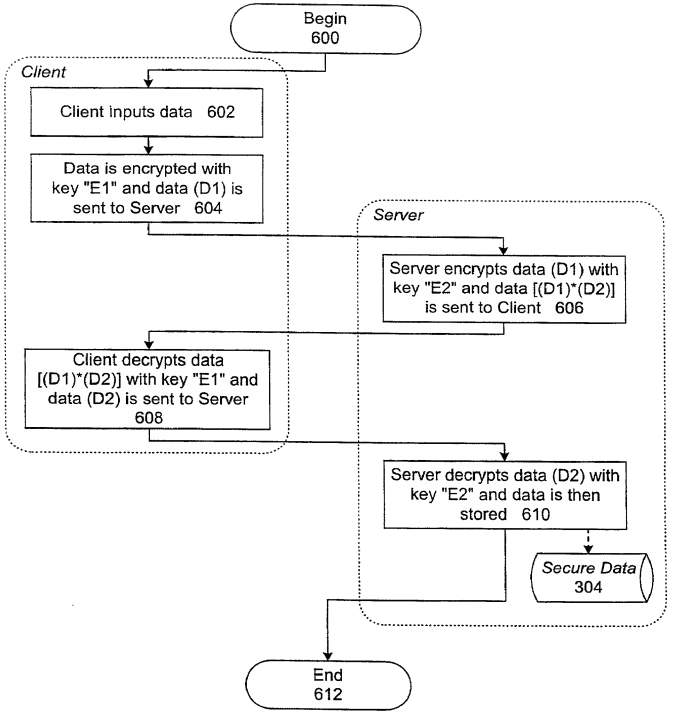
Begin
600
Client
Client inputs data 602
Data is encrypted with key "E1" and data (D1) is sent to Server 604
Server
Server encrypts data (D1) with key "E2" and data [(D1)*(D2)] is sent to Client 606
Client decrypts data [(D1)*(D2)] with key "E1" and data (D2) is sent to Server 608
Server decrypts data (D2) with key "E2" and data is then stored 610
Secure Data
304
End
612

FIG. 6

ATTORNEY'S DOCKET NO.: PA1066US

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **"System and Method of Sending and Receiving Secure Data Using Anonymous Keys,"** the specification of which (check one):

[ ] is attached hereto.
[X] was filed on October 14, 1999
as U.S. Application No. _____
or PCT International Application No. PCT/US99/24191
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year filed)	Yes	No
(Number)	(Country)	(Day/Month/Year filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Application Number)	(Filing Date)	(Status -- patented, pending, abandoned)
PCT/US99/24191	October 14, 1999	Pending
(Application Number)	(Filing Date)	(Status -- patented, pending, abandoned)

POWER OF ATTORNEY: I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

John S. Ferrell, Reg. No. 34,593; J. Eppa Hite, Reg. No. 30,266;
Gregory J. Koerner, Reg. No. 38,519; Charles B. Katz, Reg. No. 36,564;
John D. Henkhaus, Reg. No. 42,656; Susan Yee, Reg. No. 41,388;
Robert Toczycki, Reg. No. 38,341 and Aaron Wininger, Reg. No. 45,229.

SEND ALL CORRESPONDENCE TO:

Aaron Wininger
CARR & FERRELL *LLP*
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
TEL: (650) 812-3400
FAX: (650) 812-3444

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor: Lynn Spraggs

Inventor's signature _____ Dated: 3/28/2000

Residence 8604 Kalavista Dr

Post Office Address Vernon B.C. Can Citizenship Canadian